ICS 35.240
CCS L70

团　　体　　标　　准

T/ISC0147—2026

能源管理解决方案能力要求

Capability requirements for energy management solutions

（发布稿）

2026-09-08 发布　　2026-10-08 实施

中 国 互 联 网 协 会　　发 布

目次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、施耐德电气（中国）有限公司、中国煤矿机械装备有限责任公司、中国煤矿机械装备有限责任公司北京技术服务分公司、北京华宇信息技术有限公司、京东科技信息技术有限公司、中移（苏州）软件技术有限公司、联想（北京）有限公司、北京联华信科技有限公司、北京交通大学、本相空间（珠海）科技有限公司、上海华讯网络系统有限公司、北京邮电大学、华中科技大学、形意象（珠海）科技有限公司、政达研学（雄安）科技有限公司。

本文件主要起草人：徐恩庆、谭坦、刘冠军、姬海南、王璇、王振宇、崔超、张圣千、卞博文、何川、黄伟伦、王挺、刘岩、张尚雷、王江、李雪、董军华、鲍宁、张创伟、张翔清、贺皓、韩冬、张麒、胡建华、闫超众、章华丽、冉晔、宋吉晓、任婷、卞旭东、吴凯、张文祥、宋冲冲、吴佳兴、宋光通、吴宁、石子豪、高源、李梦远、包梓淇、常博然、陈凯南、于跃、孔令麒、吕晓冬、崔海澎、李天资、苏蕾权、陈金涛、赖雪、李婷婷。

引　言

随着物联网、大数据、人工智能、边缘计算等技术在能源领域的快速发展和深度应用，能源管理系统的综合能力面临全方位、体系化的新要求。当前，我国能源管理领域仍存在多源异构数据集成难、核心技术自主水平亟待提升、产业生态协同效率不高、安全风险防范体系不完善等挑战，亟须建立统一、规范的能力要求标准，引导产业健康有序发展。

本文件立足能源管理行业相关国家标准和行业规范，结合当前能源管理行业数字化转型趋势、技术发展现状及行业实践经验，旨在规范能源管理行业解决方案架构设计，明确各部署版本的技术要求、核心组件、部署流程及合规标准，提升解决方案的统一性、兼容性和可落地性，助力行业实现多源能源数据协同、能耗精准管控、能效持续优化，支撑“双碳”目标落地和能源数字化转型。

本文件注重GB/T 29456—2025《能源管理体系实施、保持和改进GB/T 23331能源管理体系指南》等国家标准和能源相关法律的衔接，遵循“权威性、通用性、可落地性、前瞻性”原则，适用于工业、建筑、园区、公共机构等各类能源管理场景，为行业内企业、科研机构及相关单位开展方案架构设计、选型、部署、运维提供标准化依据。

本文件明确了能源管理行业解决方案的能力要求。

对本文件中的具体事项，法律法规另有规定的，应遵守其规定执行。

能源管理解决方案能力要求

1 范围

本文件规定了能源管理解决方案的总体架构、技术要求、部署与运维要求和合规性要求。

本文件适用于能源管理解决方案的架构设计、方案选型、部署实施、运行维护和合规检测。适用场景包括工业企业、商业建筑、产业园区、公共机构和居民社区，能源类型包括电力、水、燃气、热力和可再生能源。适用主体包括能源管理解决方案提供商、用能单位、科研机构、检测认证机构、行业监管部门及相关从业人员。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 778（所有部分） 饮用冷水水表和热水水表

GB/T 17215（所有部分） 交流电测量设备

GB/T 20281 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 21028 信息安全技术 服务器安全技术要求

GB/T 21671 基于以太网技术的局域网（LAN）系统验收测试方法

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 23331—2020 能源管理体系 要求及使用指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

能源管理 energy management

以提升能源利用效率、降低能源消耗、优化能源结构与调度分配、保障能源安全与品质为目标，通过数据采集、分析、管控、优化等手段，对各类能源（电力、水、燃气、热力、可再生能源等）的生产、传输、存储、消耗全流程进行统筹管理的活动，同时适配“双碳”目标下的碳排放监测与管控需求。

3.2

能源管理解决方案架构 energy management solution architecture

为实现能源管理目标，整合硬件、软件、网络、数据、安全等各类资源，明确各组件的功能边界、交互逻辑、技术标准及部署方式，形成的分层、模块化、可扩展的整体架构设计方案。

3.3

多源能源数据 multi-source energy data

来源于不同能源类型、不同采集终端、不同用能环节的数据，包括电力数据（电压、电流、功率等）、水数据（用水量、水压等）、燃气数据（用气量、气压等）、热力数据（供热量、温度等）及设备运行数据、环境数据等。

3.4

能效优化 energy efficiency optimization

基于能源数据采集与分析，识别能源浪费环节，通过设备管控、运行调整、策略优化等手段，提升能源利用效率，降低能源消耗的过程。

3.5

数据本地化存储 local data storage

将能源数据、设备数据、用户数据等存储在用能单位本地或国家规定的本地存储设施中，不擅自传输至境外或非指定云端的存储方式，符合数据安全合规要求。

3.6

边缘计算 edge computing

在靠近感知层设备或数据采集源头的边缘节点，实现数据预处理、协议转换、本地缓存、简单分析及管控指令下发的计算模式，可降低数据传输压力，提升系统响应速度。

3.7

云原生应用 cloud-native application

基于云计算架构设计开发，适配云端弹性扩展、按需部署特性，支持容器化部署、微服务架构的应用程序，具备轻量化、可复用、易扩展的特点。

3.8

多可用区部署 multi-availability-zone deployment

云部署场景下，将云资源（云服务器、云数据库等）部署在云端不同可用区（地理位置独立、基础设施隔离的区域），实现故障隔离和容灾备份，提升系统高可用性。

3.9

能源品质 energy quality

能源供应在满足用能设备正常运行要求的技术特性。能源品质劣化可能导致设备效率下降、寿命缩短或故障。

3.10

能源调度与分配 energy dispatch and allocation

基于能源供需预测、设备状态、价格信号等约束，通过优化算法决定各类能源在时空上的流向、比例和强度的管理活动，旨在提升综合能效、降低用能成本、保障供应可靠性。

4 缩略语

下列缩略语适用于本文件

AI： 人工智能(Artificial Intelligence)

CPU： 中央处理器(Central Processing Unit)

CSV： 逗号分隔值(Comma-Separated Values)

DDoS： 分布式拒绝服务(Distributed Denial of Service)
ECS： 弹性云服务器(Elastic Compute Service)
HDD： 机械硬盘/硬盘驱动器(Hard Disk Drive)
IDS： 入侵检测系统(Intrusion Detection System)
IP： 互联网协议(Internet Protocol)
IPS： 入侵防御系统(Intrusion Prevention System)
JSON：JavaScript对象表示法（JavaScript Object Notation）
K3s：轻量级 Kubernetes 发行版（K3s）
K8s： 开源容器编排引擎(Kubernetes)
LoRa： 远距离无线电(Long Range Radio)
Modbus：串行通信协议（Modbus）
MQTT： 消息队列遥测传输协议(Message Queuing Telemetry Transport)
OPC UA： 开放平台通信统一架构(Open Platform Communications Unified Architecture)
OSS： 对象存储服务(Object Storage Service)
PDF： 便携式文档格式(Portable Document Format)
PLC： 可编程逻辑控制器(Programmable Logic Controller)
RAID： 独立磁盘冗余阵列(Redundant Array of Independent Disks)
RS-485： 串行通信标准485(Recommended Standard 485)
SM4： 商用密码算法4/国密分组密码算法(ShangMi 4)
SSD： 固态硬盘(Solid State Drive)
SSL： 安全套接层(Secure Sockets Layer)
SSO： 单点登录(Single Sign-On)
TLS： 传输层安全(Transport Layer Security)
UPS： 不间断电源(Uninterruptible Power Supply)
USB： 通用串行总线(Universal Serial Bus)
VLAN： 虚拟局域网(Virtual Local Area Network)
VPN： 虚拟专用网络(Virtual Private Network)
Wi-Fi： 无线保真(Wireless Fidelity)
XML： 可扩展标记语言(Extensible Markup Language)

5 总体架构

能源管理行业解决方案架构采用“分层设计、模块化部署、全流程安全、多场景适配”的总体思路，统一分为感知层、传输层、平台层、应用层、安全层五大层级，通常包括本地部署、云部署两种模式及单机版、高可用集群版两种形态，各层级功能边界清晰、交互逻辑明确，可根据不同用能场景、用能规模灵活选择部署模式。

图 1　能源管理行业解决方案架构

5.1　核心原则

统一性原则：各层级接口、协议、数据格式统一，确保不同组件、不同部署版本之间的兼容性和互联互通，符合国家及行业相关标准。

可扩展性原则：架构设计具备良好的扩展性，支持采集终端、功能模块、计算资源的灵活扩容，适配未来技术升级（如AI、大数据深度应用）和业务需求拓展（如跨区域集中管控、多能源协同管理）。

可靠性原则：核心组件具备冗余备份、故障自愈能力，确保系统持续稳定运行，避免因单点故障导致能源管理业务中断，高可用集群版应满足特定的可用性指标。

安全性原则：覆盖数据采集、传输、存储、处理、使用全流程安全，落实身份认证、权限管理、数据加密、漏洞防护等安全措施，符合等保合规、数据安全等相关要求。

可落地性原则：架构设计贴合行业实际应用场景，核心组件、技术规范具备可实施性，部署流程、运维规范简洁明确，便于行业内各主体落地执行，避免空泛设计。

前瞻性原则：结合能源管理行业数字化转型、“双碳”目标落地、物联网与AI融合等发展趋势，架构设计预留技术升级接口，可适配未来碳排放管控、智能能效优化、跨领域能源协同等需求。

品质保障原则：架构设计应确保从感知层到应用层全链路具备对能源品质的监测、分析、告警与优化能力，保障能源供应满足用能设备的品质要求。

5.2　总体架构分层说明

能源管理解决方案架构五大层级相互支撑、协同工作，形成完整的能源管理闭环，各层级核心定位、功能边界及交互逻辑如下：

表 1　能源管理解决方案架构分层说明

层级	核心定位	核心功能	核心组件

层级	核心定位	核心功能	核心组件
感知层	数据采集与设备感知的核心载体，负责各类能源数据、设备运行数据的实时采集、状态感知，是能源管理的基础。	包括能源计量、设备状态监测、环境数据采集等，覆盖电力、水、燃气、热力、可再生能源等各类能源类型，支持多种采集终端接入，实现用能全流程数据全覆盖。	包括智能电表、水表、燃气表、热量表等计量器具，温度、湿度、压力等传感器，PLC、变频器等智能设备，数据采集终端、边缘采集网关等，具体组件根据部署模式、应用场景灵活配置。
传输层	数据传输与指令交互的桥梁，负责将感知层采集的数据稳定、高效、安全传输至平台层，将平台层下发的管控指令（如设备启停、参数调整）传输至感知层智能设备。	数据传输、协议转换、数据缓存、传输状态监测等，支持多种传输协议，适配不同网络环境，确保数据传输的实时性、准确性，本地部署版可脱离公网运行，云部署版应依托公网或专用网络实现云端交互。	包括交换机、路由器、防火墙等网络设备，工业网关、传输模块（4G/5G、Wi-Fi、LoRa、以太网等），协议转换软件等，云部署版还应云端接入网关、VPN 设备等。
平台层	能源管理架构的核心支撑层，负责数据存储、处理、分析、调度，提供基础服务能力，支撑应用层功能落地，是连接感知层与应用层的核心枢纽。	包括数据接入与解析、数据清洗与转换、数据存储与备份、数据分析与挖掘、设备管理、资源调度等，本地部署版平台层部署在本地服务器，云部署版平台层部署在云端，具备弹性扩展能力。	本地部署版包括本地服务器、本地存储设备、数据库管理系统、数据分析引擎等；云部署版包括云服务器、云存储、云数据库、大数据分析引擎、云调度平台等。

表 1　能源管理解决方案架构分层说明（续）

层级	核心定位	核心功能	核心组件
应用层	面向用户的功能呈现层，基于平台层的服务能力，提供各类能源管理功能，满足不同用能场景、不同用户的管理需求，实现能源管理的可视化、智能化、精细化。	涵盖能耗监测、能效分析、设备管控、碳排放统计与分析、报表生成、告警预警、节能诊断、权限管理等，可根据工业、建筑、园区、公共机构等不同场景，灵活配置功能模块，适配“双碳”目标下的碳排放管控需求。	包括能耗监测模块、能效分析模块、设备管控系统、碳排放管理模块、报表管理系统、告警预警系统、用户管理系统等，支持 Web 端、移动端、大屏端多终端展示与操作。
安全层	覆盖整个能源管理架构的安全防护体系，负责保障系统组件、设备、数据的全流程安全，防范安全风险，确保能源管理业务安全稳定运行，符合相关合规要求。	包括身份认证、权限管理、数据加密（传输加密、存储加密）、漏洞防护、入侵检测、安全审计、数据脱敏等，覆盖感知层、传输层、平台层、应用层的所有组件和数据，明确安全责任边界。	包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、加密设备、身份认证设备、安全审计系统、数据脱敏工具等，云部署版还应云安全产品（如云防火墙、云安全中心）。

5.3 架构交互逻辑

参考框架图，共有感知层、传输层、平台层、应用层和安全层5层，其中本地部署版的所有交互均在本地环境完成，不依赖公共互联网（以下简称“公网”）；云部署版的感知层与云平台层、应用层与云平台层的交互，通过公网或专用网络完成，依托云安全产品保障交互安全，各层间的交互逻辑如下：

感知层通过各类采集终端、传感器采集能源数据、设备运行数据，经本地预处理后，通过传输层的网络设备和传输协议，传输至平台层；

平台层对接收的数据进行清洗、转换、存储，通过数据分析引擎进行能耗分析、能效评估、设备状态诊断等处理，生成分析结果和管控指令；

应用层调用平台层的分析结果和服务能力，通过多终端向用户展示能耗数据、能效指标、设备状态等信息，接收用户操作指令（如设备管控、报表查询）；

平台层根据应用层的用户指令或预设策略，生成管控指令，通过传输层传输至感知层的智能设备，实现设备启停、参数调整等管控操作，形成能源管理闭环；

安全层对上述全流程进行安全防护，对数据采集、传输、存储、处理、使用进行加密和审计，对系统组件和设备进行安全监测，防范入侵、数据泄漏等安全风险。

6 技术要求

6.1 部署要求

a） 应支持本地单机版、本地高可用集群版部署方式。
b） 应支持云单机版、云高可用集群版部署方式。

6.2 功能通用要求

所有部署版本应实现核心功能闭环，同时根据部署形态差异化适配，核心通用功能要求如下：
a） 数据采集功能：应支持电力、水、燃气、热力、可再生能源等多类型能源数据采集，支持高频/低频采集配置，具备离线缓存、断网续传、数据防篡改能力。
b） 数据处理功能：应支持数据清洗、转换、校验、聚合，能够剔除无效数据、冗余数据，确保数据准确性，适配时序数据、结构化数据的不同处理需求。
c） 能耗监测功能：应支持实时能耗监控、历史能耗查询、能耗对比分析（同比、环比、同类型用能单位对比），提供图表、数字、大屏等多形式可视化展示。
d） 能效分析功能：应支持单位产品能耗、单位面积能耗等核心能效指标计算，能够识别节能潜力，生成能效分析报告，适配“双碳”目标下的能效优化需求。
e） 设备管控功能：应支持智能设备远程启停、参数调整，具备手动控制、自动控制（基于预设策略）两种模式，实时反馈设备运行状态，支持故障告警。
f） 碳排放管理功能：应支持碳排放数据采集、核算（依据国家及行业核算标准）、统计分析，生成碳排放报表，适配碳达峰、碳中和相关管理需求。
g） 告警预警功能：应支持能耗异常、设备故障、安全风险等多类型告警，可配置告警阈值、告警方式，具备告警分级、告警处理、告警记录追溯能力。
h） 报表管理功能：应支持生成日报、月报、季报、年报，以及自定义报表，报表内容涵盖能耗、能效、碳排放、设备运行等核心数据，支持导出、打印、自动推送。
i） 用户管理功能：应支持多用户、多角色分级管理，配置不同权限（如查看权限、操作权限、管理权限），具备操作日志审计、身份认证能力。
j） 混合能源切换与转换功能：对于存在两种及以上能源类型的用能场景，系统应支持：
（1）手动或自动切换：根据预设策略（如电价时段、储能荷电状态、可再生能源出力）自动切换主用能源来源；
（2）无缝转换：切换过程中关键负荷的供电或供能不中断，电压和频率波动不超过设备允许范围；（3）切换策略配置：允许用户配置切换条件、切换顺序和回切策略；
（4）切换记录与审计：每次切换操作生成日志，包含触发条件、切换时间、结果及能源替代比例。

6.3 性能通用要求

各部署版本的核心性能指标及指标值应符合附录B的规定
a） 数据准确性：应保证数据采集、传输和处理的准确性。
b） 系统响应性：应满足核心业务和复杂业务的响应要求。
c） 可靠性：高可用部署版本应具备冗余和故障切换能力。
d） 可扩展性：应支持采集终端、用能点位、功能模块的灵活扩展，扩展过程不影响现有业务正常运行。

6.4 安全通用要求

安全要求覆盖全架构、全流程，遵循“分级防护、纵深防御”原则，核心要求如下：

a） 身份认证：应支持多因素认证（账号密码、短信或电子邮件验证、硬件认证中的至少两种认证因素），用户与设备均应通过身份认证后方可接入系统。

b） 权限管理：应遵循最小权限原则，实现用户、角色、资源的精细化权限分配，支持权限动态调整与回收。

c） 数据安全：数据传输应采用SSL/TLS 、国密等加密算法，数据存储采用加密存储，敏感数据应进行脱敏处理，数据访问、传输、使用全程留痕。

d） 设备安全：感知层、传输层设备应具备防篡改、抗干扰能力，支持固件升级、漏洞修复，云端设备具备DDoS防护、入侵检测能力。

e） 安全审计：应具备全流程安全审计能力，审计日志包含用户操作、数据访问、设备接入、故障切换等内容，日志存储时间≥6个月（高可用版本≥1年），支持审计报告生成与追溯。

f） 合规适配：应符合GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》，本地部署版至少应满足等保二级，云高可用集群版至少满足等保三级。

6.5 兼容性通用要求

a） 协议兼容性：应支持Modbus、OPC UA、MQTT等主流工业通信协议，确保不同厂商的感知层、传输层设备可互联互通。

b） 软硬件兼容性：软件组件应适配主流操作系统（Windows Server、Linux、Android、iOS），硬件组件应支持标准化接口（RS-485、以太网、USB等），不同部署版本的核心组件可实现平滑升级与迁移。

c） 数据兼容性：应支持主流数据格式（JSON、CSV、XML、时序数据格式），不同系统之间的数据交互具备一致性，支持历史数据的导入、导出与迁移。

7 服务要求

本文件针对本地部署版、云部署版的共性特点，制定统一的部署与运维通用要求，各部署版本的专项部署、运维要求已在对应章节明确，本章节为通用约束。

7.1 部署通用规范

7.1.1 部署准备

a） 应具备规划部署能力：应拥有至少一项已落地实施的同类项目案例，能够基于项目经验开展现场勘查，明确用能点位分布、网络环境、机房条件（本地部署）、云平台选型（云部署）等核心信息，输出现场勘查记录及可实施的部署方案。

b） 采购校验规范性：应完成组件采购与校验，参照已落地项目的采购清单与验收标准，确保所有硬件、软件组件符合本文件的技术要求与配置标准，出具组件校验报告。

c） 部署人员培训体系完整性：应具备已落地项目的培训经验，建立部署人员培训机制，对部署人员进行技术培训，内容涵盖部署流程、安全规范、故障处理预案，并形成培训教材库与考核记录。

7.1.2 部署实施

a） 实施流程规范性：应严格按照部署实施方案执行，遵循“先硬件后软件、先本地后云端、先调

试后上线”的原则，完整记录部署过程，形成可追溯的实施日志。

b） 安全操作严谨性：部署过程中应落实安全防护措施，防范设备损坏、数据泄露、网络中断等风险，核心环节（如加密配置、权限分配）应执行双人复核，并形成可验证的复核记录。

7.1.3 部署验收

a） 验收测试全面性：部署完成后，应按照本文件规定的性能指标、功能要求，开展覆盖全业务流程的验收测试，出具包含测试用例与测试结论的验收测试报告。

b） 移交验收规范性：验收合格后，应与用能单位完成组件移交、运维交底，签订部署验收协议，完整交付操作手册、运维手册、故障处理预案等资料，形成资料移交清单。

7.2 运维通用规范

7.2.1 运维组织

a） 责任界定清晰性：应明确运维责任主体，本地部署版以用能单位为主、解决方案提供商为辅；云部署版以解决方案提供商联合云平台服务商为主、用能单位为辅，并形成书面责任矩阵。

b） 沟通机制有效性：应建立运维沟通机制，设立专属运维对接人，确保故障、需求能够快速传达与响应，保留沟通及处理过程记录。

7.2.2 运维保障

a） 工具配备完备性：应配备必要的运维工具（如故障排查工具、固件升级工具、数据备份工具），云端运维应具备自动化运维平台，本地运维应配备基础检修工具，并验证工具可用性。

b） 知识库实用性：应建立运维知识库，收录常见故障处理方案、操作指南、版本更新记录等内容，实现运维经验沉淀与复用，并具有持续更新机制。

7.2.3 升级与迭代

a） 升级计划可预见性：解决方案提供商应定期发布软件版本更新、硬件固件升级计划，明确升级内容、升级时间、回滚方案，并提前告知用能单位。

b） 升级过程可控性： 升级迭代应遵循“灰度升级、风险可控”原则，避免对用能单位的能源管理业务造成影响，升级后应开展功能与性能验证，形成升级验证记录。

8 合规性要求

能源管理解决方案架构的设计、部署、运维全流程，在符合法律法规和行业标准合规的背景下，应满足安全等级合规、数据管理合规2类合规性要求，确保解决方案的合法性、规范性和安全性。

8.1 安全等级合规

a） 应具备等保适配能力：所有部署版本的安全防护能力不低于网络安全等级保护二级要求；核心用能单位、云高可用集群版达到等级保护三级要求。

b） 应具备云安全合规能力：云部署版支持接入云安全能力，符合云安全相关行业标准，具备第三方权威机构出具的安全检验与认证证书，确保云端资源与数据安全。

c） 应具备等保测评能力，定期开展等级保护测评，测评不合格的在规定期限内完成整改，形成完整的自测机制并提供相关报告或证明文件，以确保持续符合安全等级要求。

8.2 数据管理合规

a） 应具备采集合规能力：数据采集应符合能源计量相关标准，采集行为与采集范围可通过标准规范及日志记录进行核验，确保数据合法、准确，不采集与能源管理无关的敏感数据（如个人生物识别信息）。

b） 应具备存储合规能力：数据存储应遵循数据本地化要求，核心能源数据、碳排放数据存储于中国大陆境内服务器，存储位置与存储行为可核查验证，不擅自向境外传输。

c） 应具备使用合规能力：数据使用应遵循“合法、正当、必要”原则，数据使用行为、授权记录可追溯、可验证，未经用能单位授权，不向第三方泄露、出售、使用能源数据。

d） 应具备全生命周期管理能力：应建立并执行数据全生命周期管理制度，各环节流程、操作记录与责任主体可追溯、可核查；数据销毁符合相关规范要求，销毁结果可验证、不可恢复。

附录 A
（资料性）
部署版本选型

表 A.1　部署版本选型表

选型维度	本地单机版	本地高可用集群版	云单机版	云高可用集群版
用能规模	小型（点位≤50）	中大型（点位≥500）	小型（点位≤30）	中大型（点位≥500）
用能点位分布	集中	集中	分散	分散/跨区域
高可用需求	低 （允许短期中断）	极高 （核心业务不中断）	低 （允许短期中断）	极高 （核心业务不中断）
数据本地化要求	高	极高	低	中 （混合云可适配）
本地机房条件	有 （简易机房）	有 （标准机房）	无	无
运维能力要求	基础 （普通人员）	专业 （运维团队）	基础 （普通人员）	云端专业/ 本地基础
适用核心场景	小型工厂、 社区服务中心	大型工业企业、 核心能源站点	连锁商铺、 临时用能	集团企业、 跨区域园区

附录 B
（规范性）
各部署版本核心性能指标

表 B.1　核心性能指标对比

性能指标	本地单机版	本地高可用集群版	云单机版	云高可用集群版
年可用性	-	≥99.98%	-	≥99.98%
故障切换延迟	-	≤60 秒	-	≤30 秒（节点）/ ≤60 秒（可用区）
并发数据写入速率	≥500 条/秒	≥10000 条/秒	≥1000 条/秒	≥50000 条/秒
并发用户数	≤20 人	≤200 人	≤30 人	≤500 人
断网缓存时间	≥7 天	≥15 天	≥7 天	≥30 天
数据备份成功率	≥99.9%	≥99.99%	≥99.9%	≥99.999%

附录 C
（规范性）
合规检测核心要点

C.1　架构合规

应核查解决方案是否符合本文件规定的分层设计和模块化部署要求，并确认各部署版本的组件配置是否符合相应条款。

C.2　功能合规

应按照第6章的规定核查各项功能，并记录核查依据和结果。

C.3　性能合规

应核查对应部署版本的性能指标，并记录测试条件、测试数据和判定结果。

C.4　安全合规

应核查等级保护、数据加密、身份认证和安全审计措施是否符合本文件的规定。

C.5　数据合规

应核查数据采集、存储、传输和使用过程是否符合适用的法律法规及本文件的规定。

附录 D
（规范性）
本地部署方案部署能力要求

本地部署版核心特点：所有核心组件（硬件、软件、数据库等）均部署在用能单位本地环境，数据存储、处理、管控均在本地完成，无公网依赖，具备数据本地化、自主管控、低延迟的优势，适用于对数据安全性、自主管控能力要求较高，且不便于接入公网的用能场景。

本地部署版架构遵循总体架构的分层设计原则，重点强化数据本地化存储、本地自主管控、离线运行支持等能力，感知层、传输层、平台层、应用层、安全层均部署在本地，各层级组件适配本地环境，确保系统稳定运行和数据安全，同时符合GB/T 23331—2020、《能源行业数据安全管理办法（试行）》等相关标准要求。

D.1 本地部署版总体架构

本地部署版总体架构分为感知层、传输层、本地平台层、应用层、安全层五大层级，各层级组件均部署在用能单位本地机房或指定区域，无云端组件，交互逻辑遵循总体架构要求，重点优化本地数据处理、离线运行、自主管控能力，具体架构如下：

感知层：部署在用能现场，覆盖所有用能点位和设备，采集各类能源数据和设备运行数据，支持离线缓存，确保断网情况下数据不丢失；

传输层：采用本地局域网、工业总线等传输方式，不依赖公网，部署本地网络设备和传输网关，实现感知层与本地平台层的数据传输和指令交互，具备传输状态监测和故障自愈能力；

本地平台层：部署在本地服务器和存储设备，负责本地数据存储、处理、分析和资源调度，具备数据备份、本地计算、离线运行等能力，支撑应用层功能落地；

应用层：部署在本地服务器，支持Web端、本地终端展示，提供各类能源管理功能，用户通过本地终端访问和操作，实现能源管控和数据分析；

安全层：部署本地安全设备和安全软件，覆盖本地所有组件和数据，落实本地安全防护措施，实现自主安全管控，符合等保合规要求。

D.2 本地部署版核心组件

本地部署版核心组件包括硬件组件、软件组件两大类，所有组件均应符合国家及行业相关技术标准，具备兼容性、可靠性、可维护性，明确组件配置要求和兼容性规范，具体如下：

D.2.1 硬件组件

硬件组件部署在用能单位本地，包括感知层硬件、传输层硬件、本地平台层硬件、安全层硬件，具体组件及技术标准、配置要求如下：

感知层硬件：

计量器具：智能电表（精度≥0.5级）、水表（精度≥2级）、燃气表（精度≥1.5级）、热量表（精度≥2级）等，应符合 GB/T 17215（所有部分）和 GB/T 778（所有部分）的规定，支持数据本地缓存和离线上传，具备防篡改功能；

传感器：温度传感器（精度±0.5℃）、湿度传感器（精度±5%RH）、压力传感器（精度±0.5%FS）等，适配工业、建筑等不同场景的环境要求，支持4 mA～20 mA、RS-485等输出信号；

智能设备：PLC、变频器、智能控制器等，支持Modbus、OPC UA等工业协议，具备远程管控（本地）、状态反馈功能，符合工业设备相关标准；

采集终端：数据采集仪、边缘采集网关等，支持多协议接入，具备数据预处理、本地缓存（缓存容量≥16GB）、断网续传功能，适配本地传输环境。

传输层硬件：

网络设备：交换机（千兆端口≥8个，支持VLAN划分）、路由器（支持静态路由，具备防火墙功能），应符合 GB/T 21671 的规定，适配本地局域网传输；

传输网关：工业网关（支持Modbus、OPC UA、MQTT等协议转换），具备数据加密传输功能，支持本地缓存，适配工业总线和局域网传输；

传输模块：以太网模块、RS-485总线模块等，确保数据传输速率≥100 Mbit/s，传输延迟≤100 ms，传输成功率≥99.9%。

本地平台层硬件：

服务器：根据部署形态（单机/集群）配置，单机版服务器配置：CPU≥8核，内存≥16GB，硬盘≥1TB（SSD）；集群版节点服务器配置：CPU≥16核，内存≥32GB，硬盘≥2TB（SSD），支持冗余部署，应符合 GB/T 21028 的规定；

存储设备：磁盘阵列（集群版必备）、本地硬盘（单机版），存储容量根据数据量确定，应满足至少1年的历史数据存储需求，支持RAID备份，存储速率≥500 MB/s；

接口设备：串口服务器、USB接口模块等，支持多接口扩展，适配不同组件的接口需求，确保组件互联互通。

安全层硬件：

防火墙：支持包过滤、入侵检测、VPN等功能，适配本地局域网环境，具备日志审计功能，应符合GB/T 20281 的规定；

加密设备：数据加密机（支持国密算法SM4），负责数据存储和传输加密，符合国家密码相关标准；

身份认证设备：USB Key、指纹认证器等，用于用户身份认证，支持多用户分级认证，确保系统访问安全。

D.2.2 **软件组件**

软件组件部署在本地服务器，包括数据采集软件、平台软件、应用软件、安全软件，具体组件及技术标准、配置要求如下：

数据采集软件：支持Modbus、OPC UA、MQTT等工业协议，具备多终端接入、数据预处理、数据清洗、离线缓存、断网续传功能，采集频率可配置（1 min～1 h），数据采集准确率≥99.8%；

平台软件：

数据库管理系统：支持关系型数据库（MySQL、PostgreSQL等）和时序数据库（InfluxDB、TimescaleDB等），时序数据库用于存储能源时序数据，支持高并发写入，写入速率≥1000条/秒；

数据分析引擎：支持能耗统计、能效分析、设备故障诊断、碳排放核算等功能，具备本地计算能力，分析延迟≤5秒，支持自定义分析模型；

应用软件：

能耗监测软件：支持实时能耗监测、历史能耗查询、能耗对比分析、能耗报表生成等功能，可视化展示用能数据；

能效优化软件：支持能效指标计算、节能潜力分析、节能策略推荐等功能，适配“双碳”目标下的能效管控需求；

设备管控软件：支持智能设备的启停、参数调整、状态反馈等功能，具备手动控制和自动控制两种模式；

碳排放管理软件：支持碳排放数据采集、统计、分析、报表生成等功能，适配“双碳”目标下的碳排放管控需求；

用户管理软件：支持多用户分级管理、权限分配、操作日志审计等功能，符合安全管理要求。

安全软件：

杀毒软件：支持本地病毒查杀、实时监控，定期更新病毒库，适配工业环境；

安全审计软件：支持系统操作日志、数据访问日志、传输日志的采集、存储和审计，日志存储时间≥6个月；

漏洞扫描软件：支持定期对本地组件、软件进行漏洞扫描，生成漏洞报告和修复建议，符合等保合规要求。

D.2.3 组件兼容性要求

硬件组件兼容性：所有硬件组件应支持统一的接口标准（如RS-485、以太网、USB等），感知层硬件与传输层硬件、传输层硬件与本地平台层硬件应适配，确保数据传输和指令交互顺畅；服务器、存储设备应支持硬件冗余，集群版节点硬件配置需一致；

软件组件兼容性：所有软件组件应适配本地操作系统（如Windows Server、Linux等），数据采集软件与数据库管理系统、数据分析引擎应适配，平台软件与应用软件应支持统一的接口协议，安全软件需与其他软件兼容，不影响系统正常运行；

软硬件兼容性：软件组件应适配本地硬件组件，数据库管理系统、数据分析引擎应适配服务器和存储设备的性能，确保系统运行流畅，无卡顿、崩溃等问题；

协议兼容性：所有组件应支持Modbus、OPC UA、MQTT等主流工业协议，协议版本需统一，确保不同厂商、不同类型的组件互联互通，符合GB/T 23331—2020 的规定。

D.3 本地单机版（本地单机部署）

本地单机版是本地部署版的单机形态，核心特点：仅部署一套核心硬件（服务器、采集终端等）和软件组件，承担所有数据采集、处理、管控、存储功能，无冗余备份和故障切换能力，架构简单、部署成本低、维护便捷，适用于小型用能单位、简易能耗监控场景。

D.3.1 架构拓扑

本地单机版架构拓扑简洁，所有组件集中部署，具体拓扑如下：

用能现场感知层（计量器具、传感器、智能设备、采集终端）→ 传输层（本地交换机、路由器、传输网关）→ 本地单机服务器（部署平台软件、应用软件、数据库）→ 本地终端（Web端、本地电脑）；安全层硬件（防火墙）、安全软件部署在单机服务器和传输层，覆盖整个系统；所有组件通过本地局域网连接，无冗余节点，数据存储在单机服务器本地硬盘，不依赖公网，支持离线运行。

D.3.2 硬件配置标准

本地单机版硬件配置应满足小型用能场景的需求，兼顾性价比和可靠性，具体配置标准如下：

服务器：CPU≥8核（Intel Xeon E3或同等性能），内存≥16GB DDR4，硬盘≥1TB SSD + 2TB HDD（SSD用于系统和数据库，HDD用于历史数据存储），支持单电源（可选冗余电源），具备散热、防尘功能，适配本地机房环境；

感知层硬件：根据用能点位数量配置，采集终端≤5台，计量器具≤50台，传感器≤30个，智能设备≤10台，采集终端缓存容量≥16GB（），支持断网缓存；

传输层硬件：交换机1台（千兆端口≥8个，支持VLAN划分），路由器1台（支持静态路由，具备基础防火墙功能），传输网关1台（支持多协议转换），传输模块根据采集终端数量配置；

安全层硬件：防火墙1台（支持包过滤、入侵检测，适配本地局域网），身份认证设备≤5个（USB Key或指纹认证器）；

其他硬件：串口服务器1台（支持≥4个串口），UPS电源1台（续航≥2小时，保障断电情况下系统正常运行）。

D.3.3 软件部署流程

本地单机版软件部署流程简洁，可落地性强，具体流程如下：

部署准备：完成本地单机服务器、网络设备、安全设备的硬件安装和调试，确保硬件连接正常；安装操作系统（Windows Server 或Linux），配置本地局域网，设置服务器IP地址（静态IP）；

数据库部署：在单机服务器上安装数据库管理系统（MySQL 或PostgreSQL）和时序数据库（InfluxDB或TimeScaleDB），配置数据库参数，创建能源管理相关数据库和数据表，设置数据库备份策略（每日自动备份）；

平台软件部署：安装数据分析引擎、数据采集软件，配置软件参数，对接数据库，设置数据采集协议、采集频率，调试数据采集功能，确保感知层数据可正常接入；

应用软件部署：安装能耗监测软件、能效优化软件、设备管控软件、用户管理软件等应用组件，配置应用参数，对接平台软件，调试应用功能，确保各功能模块正常运行；

安全软件部署：安装杀毒软件、安全审计软件、漏洞扫描软件，配置安全参数，更新病毒库和漏洞库，设置安全审计规则，开启实时监控功能；

系统调试：整体调试系统，测试数据采集、传输、存储、分析功能，测试应用功能和安全防护功能，排查故障，确保系统运行流畅；

用户培训：对用能单位相关人员进行系统操作培训，包括数据查看、设备管控、报表生成、故障处理等，提供操作手册；

部署验收：按照本文件规定的测试标准和验收规范，完成部署验收，出具验收报告，验收合格后系统正式投入使用。

D.3.4 适用场景

本地单机版适用于用能规模小、用能点位少、数据量小、无高可用需求，且对数据本地化、自主管控有一定要求，不便于接入公网的场景，具体包括：

小型工业企业（如小型加工厂、作坊），用能点位≤50个，日均数据量≤10万条；

小型商业建筑（如小型商铺、写字楼底商），用能类型单一（如仅电力），无复杂设备管控需求；

小型公共机构（如社区服务中心、小型学校），用能规模小，仅需基础能耗监测功能；

简易能耗监控场景（如单一设备能耗监测、临时用能场景），无高可用需求，预算有限；

对网络依赖度低，无公网接入条件，且需要自主管控数据的小型用能单位，符合《能源行业数据安全管理办法（试行）》中数据本地化存储要求。

D.3.5 维护要求

本地单机版维护便捷，维护成本低，具体维护要求如下：

日常维护：安排专人负责日常维护，每日检查系统运行状态、数据采集状态，查看设备运行日志和安全日志，排查异常情况；每周清理服务器缓存，检查硬盘存储空间，确保存储空间充足；

定期维护：每月检查硬件设备（服务器、网络设备、采集终端）的运行状态，清理设备灰尘，检查线路连接；每月更新杀毒软件病毒库、漏洞扫描软件漏洞库，进行一次全面病毒查杀和漏洞扫描；每季度对数据库进行一次全量备份，测试备份数据恢复功能；每年对硬件设备进行一次全面检测和维护，更换老化部件；

故障维护：建立故障应急处理机制，接到故障报警后，维护人员需在2小时内响应，4小时内完成故障排查和修复（简单故障）；复杂故障（如服务器崩溃）应联系技术支持，24小时内完成修复；故障修复后，应记录故障原因、处理过程和结果，形成故障报告；

软件维护：定期更新平台软件、应用软件版本，修复软件漏洞，优化软件性能；根据用户需求，适时调整软件参数和功能配置；

数据维护：定期清理无效数据、冗余数据，确保数据准确性和完整性；每年对历史数据进行一次归档，归档数据可存储在外部硬盘，保留至少3年。

D.3.6 局限性

本地单机版受限于单机部署形态，存在以下局限性，不适用于中大型用能场景和高可用需求场景：

无冗余备份：仅部署一套核心组件，无冗余节点，一旦服务器、数据库或核心硬件出现故障，系统将全面中断，影响能源管理业务；

性能有限：并发处理能力、数据处理能力有限，无法支撑大量用能点位、海量数据的采集和分析，难以适配用能规模扩大后的需求；

扩展困难：硬件、软件组件扩展难度大，无法灵活增加采集终端、扩展功能模块，难以适配业务需求的拓展；

无负载均衡：所有数据处理、用户访问均由单机承担，长期高负载运行易导致系统卡顿、崩溃，影响系统稳定性；

维护依赖性强：系统维护依赖专人负责，维护人员应具备一定的技术能力，否则难以处理复杂故障。

D.4 高可用集群版（本地集群部署）

本地高可用集群版是本地部署版的集群形态，核心特点：部署多套核心组件（节点），通过集群管理技术实现负载均衡、故障切换、冗余备份，具备高可靠性、高可用性、高处理能力，数据存储和处理均在本地，自主管控能力强，适用于中大型用能单位、核心用能场景。

D.4.1 架构拓扑

本地高可用集群版架构拓扑采用多节点集群部署，核心组件冗余配置，具体拓扑如下：

用能现场感知层（计量器具、传感器、智能设备、采集终端）→ 传输层（本地交换机集群、路由器集群、传输网关集群）→ 本地平台层（服务器集群、存储集群、数据库集群）→ 应用层（应用服务器集群）→ 本地终端（Web端、本地电脑、大屏端）；安全层硬件（防火墙集群、加密设备集群）、安全软件部署在所有节点，覆盖整个系统；所有节点通过本地局域网和集群管理软件连接，实现负载均衡和故障切换，数据存储在存储集群，支持冗余备份，无公网依赖，支持离线运行，架构符合“云-边-端”协同的本地部署适配要求。

集群部署模式支持两种拓扑：主备模式、负载均衡模式，可根据用能场景选择：

主备模式：1台主节点、≥1台备节点，主节点承担主要业务（数据采集、处理、管控），备节点处于待命状态，主节点故障时，备节点自动切换，接管主节点业务，切换过程无人工干预；

负载均衡模式：≥3台节点（跟架构师确认我们目前是否有此架构方案），所有节点同时承担业务，集群管理软件将用户访问、数据处理任务均匀分配到各节点，实现负载均衡，单个节点故障时，其他节点自动接管其业务，不影响系统正常运行。

D.4.2 节点配置标准

本地高可用集群版节点配置应满足中大型用能场景的需求，核心节点冗余配置，具体配置标准如下（以3节点负载均衡模式为例）：

服务器集群：3台应用服务器 + 3台数据服务器，每台服务器配置：CPU≥16核（Intel Xeon E5或同等性能），内存≥32GB DDR4，硬盘≥2TB SSD + 4TB HDD，支持双电源冗余，具备散热、防尘、抗干扰功能，适配工业机房环境；

存储集群：1套磁盘阵列（存储容量≥10TB，支持RAID 5/6冗余备份），配套存储交换机2台，确保数据存储安全，支持数据实时同步；

数据库集群：3台数据库服务器，部署主从复制架构（MySQL集群）或分布式数据库（InfluxDB集群），支持数据实时同步，主节点故障时，从节点自动切换，确保数据库可用性；

感知层硬件：根据用能点位数量配置，采集终端≤50台，计量器具≤500台，传感器≤300个，智能设备≤100台，采集终端缓存容量≥32GB，支持断网缓存和集群接入；

传输层硬件：交换机集群（千兆交换机≥3台，每台千兆端口≥24个，支持VLAN划分和负载均衡），路由器集群（≥2台，支持静态路由、VPN和故障切换），传输网关集群（≥3台，支持多协议转换和冗余部署）；

安全层硬件：防火墙集群（≥2台，支持包过滤、入侵检测、入侵防御，适配本地局域网集群），加密设备≥3台（支持国密算法SM4），身份认证设备≤50个；

其他硬件：串口服务器集群（≥3台，每台支持≥8个串口），UPS电源集群（≥2台，续航≥4小时，保障断电情况下系统正常运行），集群管理设备1台（用于集群节点管理和监控）。

D.4.3 集群部署策略

本地高可用集群版部署策略重点关注负载均衡、故障切换、冗余备份，确保集群高可用性，具体部署策略如下：

节点部署：所有节点部署在用能单位本地机房，机房应满足恒温（18 ℃～25 ℃）、恒湿（40 %～60 %）、防尘、防静电要求，节点之间物理隔离，避免单点故障影响整个集群；

集群管理：部署集群管理软件（如Keepalived、Nginx Plus），配置负载均衡策略（轮询、加权轮询），实现用户访问、数据处理任务的均匀分配；配置故障检测机制，实时监测各节点运行状态（CPU、内存、硬盘、网络）；

故障切换：配置自动故障切换策略，主备模式下，主节点故障时，备节点在≤30秒内自动切换，接管主节点业务；负载均衡模式下，单个节点故障时，其他节点自动接管其业务，切换过程无人工干预，不影响用户使用和数据采集；

数据备份：采用“本地备份+集群备份”双重备份策略，数据库集群支持主从复制，数据实时同步；存储集群支持RAID 5/6冗余，确保单块硬盘故障时数据不丢失；每日自动进行全量备份，每小时进行增量备份，备份数据存储在存储集群和外部硬盘，保留至少3年；

网络部署：传输层采用双链路部署，避免单条链路故障导致数据传输中断；配置网络负载均衡，确保数据传输速率和稳定性；

软件部署：所有节点部署相同版本的平台软件、应用软件、安全软件，软件参数统一配置，确保各节点协同工作；采用批量部署工具，实现软件的统一安装和更新，提升部署效率。

D.4.4 故障切换机制

本地高可用集群版故障切换机制采用“实时监测-自动告警-自动切换-故障恢复”的闭环机制，确保故障快速处理，具体如下：

故障监测：集群管理软件实时监测各节点的运行状态（CPU使用率、内存使用率、硬盘存储空间、网络连接状态、软件运行状态），监测频率≤10秒/次；同时监测数据采集、传输、存储等业务流程，发现异常立即触发告警；

故障告警：故障发生时，系统自动发出告警（声音告警、短信告警、平台告警），告知维护人员故障节点、故障类型、故障时间，告警信息同步存储在安全日志中；

自动切换：根据集群部署模式（主备/负载均衡），自动触发故障切换流程，主备模式下，备节点接管主节点的IP地址、业务进程和数据处理任务，切换延迟≤30秒；负载均衡模式下，集群管理软件立即停止向故障节点分配任务，将未完成的任务和新任务均匀分配至其他正常节点，切换过程无感知，不影响业务连续性；

故障恢复：维护人员接到告警后，排查故障原因（如硬件故障、软件故障、网络故障），完成故障修复后，集群管理软件自动检测节点状态，确认正常后，将节点重新加入集群，分配业务任务，恢复集群完整负载能力；故障修复过程应记录在故障报告中，便于后续复盘优化。

D.4.5 适用场景

本地高可用集群版适用于用能规模大、用能点位多、数据量大、对系统可用性和自主管控能力要求极高，且不便于接入公网，或有严格数据本地化合规要求的中大型用能单位、核心用能场景，具体包括：

中大型工业企业（如制造业工厂、化工企业、冶金企业），用能点位≥500个，日均数据量≥100万条，核心生产环节依赖能源管控，不允许系统中断；

大型产业园区、工业园区，涵盖多家用能单位，用能类型复杂（电力、水、燃气、热力等），需要集中管控且自主掌握数据；

重点公共机构（如大型医院、高校、政府办公楼），用能规模大，对能源管控的连续性、可靠性要求高，且有数据本地化合规需求；

核心用能场景（如数据中心、新能源生产基地），能源管控直接影响核心业务运行，应具备高可用性、高可靠性和自主管控能力；

对网络依赖度低、无公网接入条件，或受政策限制应实现数据本地化存储，且用能规模较大、有高可用需求的用能单位，符合《能源行业数据安全管理办法（试行）》《中华人民共和国数据安全法》等相关要求。

D.4.6 维护要求

本地高可用集群版维护需重点关注集群节点协同、冗余备份、故障切换等核心环节，维护要求如下：

日常维护：安排专业维护团队负责日常维护，每日监测集群各节点运行状态、负载情况、数据传输状态，查看集群管理日志、设备运行日志和安全日志，排查异常情况；每日检查数据备份状态，确保备份正常；

定期维护：每月检查集群硬件设备（服务器、存储设备、网络设备、采集终端）的运行状态，清理设备灰尘，检查线路连接和电源状态；每月更新安全软件病毒库、漏洞库，进行一次全面病毒查杀和漏洞扫描；每季度对集群进行一次负载测试和故障切换测试，验证集群高可用能力；每季度对数据库进行一次全量备份恢复测试，确保备份数据可用；每年对硬件设备进行一次全面检测和维护，更换老化部件；

故障维护：建立分级故障应急处理机制，接到故障告警后，维护人员需在30分钟内响应，2小时内完成简单故障排查和修复；复杂故障（如集群崩溃、存储故障）需启动应急方案，4小时内完成故障修复，确保业务快速恢复；故障修复后，应记录故障原因、处理过程和结果，形成故障报告，定期复盘优化；

软件维护：定期更新集群管理软件、平台软件、应用软件版本，修复软件漏洞，优化软件性能；更新软件时应采用灰度更新策略，避免影响集群正常运行；根据用户需求，适时调整软件参数和功能配置；

数据维护：定期清理无效数据、冗余数据，对历史数据进行分层存储，确保数据准确性和完整性；每年对历史数据进行一次归档，归档数据存储在存储集群和外部备份设备，保留至少5年；定期检查数据同步状态，确保集群内数据一致。

附录 E
（规范性）
云部署版部署能力要求

E.1 云部署版总体架构

云部署版总体架构分为感知层、传输层、云平台层、应用层、安全层五大层级，其中感知层、传输层部署在本地用能现场，云平台层、应用层、安全层部署在云端，各层级交互逻辑遵循总体架构要求，重点优化云端与本地的交互效率、数据安全传输、弹性扩展能力，具体架构如下：

感知层：部署在各用能现场，覆盖所有用能点位和设备，采集各类能源数据和设备运行数据，支持本地缓存，确保断网情况下数据不丢失，适配多场景、多点位分散部署需求；

传输层：部署在本地用能现场，采用公网（4G/5G、Wi-Fi）或专用网络（VPN、专线）传输方式，部署简易网络设备和云端接入网关，实现感知层与云平台层的数据传输和指令交互，具备传输加密、状态监测和故障自愈能力；

云平台层：部署在云端，利用云计算、大数据技术提供弹性计算、海量存储、数据分析、资源调度等服务，支持按需扩容、按需付费，负责云端数据存储、处理、分析，支撑应用层功能落地，适配公有云、私有云、混合云三种部署模式（要注意审视我们的offer是否具备私有云和混合云部署能力）；

应用层：部署在云端，基于云平台层的服务能力，提供各类能源管理功能，支持Web端、移动端、大屏端多终端访问，用户通过互联网即可实现能源管控和数据分析，无需安装本地应用；

安全层：覆盖云端和本地全流程，云端部署云安全产品，本地部署简易安全设备，落实身份认证、权限管理、数据加密、漏洞防护等安全措施，确保云端资源、本地设备和全流程数据安全，符合等保合规要求。

E.2 云部署版核心组件

云部署版核心组件分为本地组件（感知层、传输层）和云端组件（云平台层、应用层、安全层）两大类，所有组件均应符合国家及行业相关技术标准、云服务相关规范，具备兼容性、可靠性、可扩展性，明确组件配置要求和兼容性规范，具体如下：

E.2.1 本地组件（感知层、传输层）

本地组件部署在各用能现场，以轻量化、易部署、易维护为核心，无需复杂硬件设施，具体组件及技术标准、配置要求如下：

感知层组件：

计量器具：智能电表（精度≥0.5级）、水表（精度≥2级）、燃气表（精度≥1.5级）、热量表（精度≥2级）等，应符合 GB/T 17215（所有部分）和 GB/T 778（所有部分）的规定，支持数据本地缓存（缓存容量≥8GB）和离线上传，具备防篡改、抗干扰功能，支持与云端接入网关对接；

传感器：温度传感器（精度±0.5℃）、湿度传感器（精度±5%RH）、压力传感器（精度±0.5%FS）等，适配工业、建筑、园区等不同场景的环境要求，支持4 mA～20 mA、RS-485、LoRa等输出信号，可直接接入采集终端；

智能设备：PLC、变频器、智能控制器等，支持Modbus、OPC UA、MQTT等工业协议，具备远程管控（云端）、状态反馈功能，符合工业设备相关标准，支持通过传输层与云端交互；

采集终端：轻量化数据采集仪、边缘采集网关等，支持多协议接入，具备数据预处理、本地缓存、断网续传、传输加密功能，适配公网和专用网络传输，体积小、功耗低，可直接部署在用能现场，无需专业机房。

传输层组件：

网络设备：小型交换机（千兆端口≥4个，支持VLAN划分）、4G/5G路由器（支持高速上网、VPN接入），适配本地用能现场环境，体积小、易部署，支持与云端建立稳定连接；

云端接入网关：核心传输组件，支持Modbus、OPC UA、MQTT等协议转换，具备数据加密（支持国密算法SM4、SSL/TLS加密）、身份认证、连接状态监测功能，支持4G/5G、以太网、LoRa等多种传输方式，确保本地数据安全传输至云端；

传输模块：4G/5G模块、Wi-Fi模块、LoRa模块等，根据用能现场网络环境配置，确保数据传输速率≥10Mbps，传输延迟≤500ms，传输成功率≥99.9%，支持流量监控和节能模式。

E.2.2 云端组件（云平台层、应用层、安全层）

云端组件部署在云端（公有云、私有云、混合云），以弹性扩展、集中管控、高安全性为核心，依托云计算技术提供服务，具体组件及技术标准、配置要求如下：

云平台层组件：

云服务器：采用弹性云服务器（ECS），支持按需扩容、按需付费，配置根据用能规模灵活调整，单机版云服务器配置：CPU≥8核，内存≥16GB，硬盘≥1TB（云SSD）；集群版云服务器配置：CPU≥16核，内存≥32GB，硬盘≥2TB（云SSD），支持多可用区部署，应符合 GB/T 21028 的规定；

云存储：采用对象存储（OSS）、云磁盘阵列等，支持海量数据存储，存储容量根据数据量按需扩容，支持数据冗余备份（多可用区备份），存储速率≥1 000 MB/s，支持数据生命周期管理；

云数据库：支持关系型云数据库（MySQL、PostgreSQL云版）和时序云数据库（InfluxDB、Prometheus云版），时序云数据库用于存储能源时序数据，

支持高并发写入（写入速率≥10000条/秒），支持主从复制、故障自动切换，确保数据可用性；

大数据分析引擎：采用云原生数据分析引擎（如Spark、Flink云版），支持能耗统计、能效分析、设备故障诊断、碳排放核算等功能，具备分布式计算能力，分析延迟≤3秒，支持自定义分析模型和AI算法集成；

云调度平台：负责云端资源（云服务器、云存储、云数据库）的调度、负载均衡、扩容缩容管理，支持自动调度和手动调度，实时监测云端资源运行状态，优化资源利用率，降低运维成本；

云网关：负责云端与本地传输层的对接，实现协议转换、数据解析、连接管理，支持大批量本地采集终端同时接入，具备数据加密、身份认证功能，确保云端与本地的稳定交互。

应用层组件：

云原生应用：所有应用组件采用云原生架构开发，支持容器化部署（Docker+K8s），适配云端弹性扩展特性，具备轻量化、可复用、易升级的特点，包括能耗监测云模块、能效优化云模块、设备管控云模块等；

能耗监测云模块：支持实时能耗监测、历史能耗查询、能耗对比分析、能耗报表生成等功能，可视化展示用能数据，支持多用能现场集中展示，用户通过Web端、移动端即可访问；

能效优化云模块：支持能效指标计算、节能潜力分析、节能策略推荐等功能，适配“双碳”目标下的能效管控需求，可结合AI算法实现智能能效优化；

设备管控云模块：支持智能设备的远程启停、参数调整、状态反馈等功能，具备手动控制和自动控制两种模式，支持多用能现场设备集中管控，实时反馈设备运行状态；

碳排放管理云模块：支持碳排放数据采集、统计、分析、报表生成等功能，适配“双碳”目标下的碳排放管控需求，可对接碳排放核算平台，生成符合规范的碳排放报表；

用户管理云模块：支持多用户分级管理、权限分配、操作日志审计等功能，支持多租户隔离（适用于多用户共享云平台场景），符合安全管理和合规要求，支持单点登录（SSO）。

安全层组件：

云防火墙：部署在云端，支持包过滤、入侵检测、入侵防御、DDoS防护等功能，适配云端环境，具备日志审计功能，可根据业务需求灵活配置安全规则，应符合 GB/T 20281 的规定；

云安全中心：负责云端资源、云应用、数据的全面安全监测，支持漏洞扫描、病毒查杀、安全告警、风险评估等功能，实时监测安全风险，生成安全报告和修复建议；

数据加密服务：采用云端数据加密服务，支持数据传输加密（SSL/TLS 1.3）、数据存储加密（国密算法SM4），支持数据脱敏、数据加密密钥管理，确保云端数据安全，符合《中华人民共和国数据安全法》相关要求；

身份认证服务：采用云端身份认证服务，支持多因素认证（账号密码+短信验证+USB Key），用于用户和本地设备的身份认证，确保云端资源和系统的访问安全；

安全审计服务：支持云端系统操作日志、数据访问日志、传输日志的采集、存储和审计，日志存储时间≥1年，可生成安全审计报告，满足等保合规要求。

E.2.3 组件兼容性要求

本地组件兼容性：本地感知层组件与传输层组件应支持统一的接口标准（如RS-485、以太网、LoRa等），采集终端与云端接入网关应适配，确保数据传输顺畅；本地组件应支持主流工业协议（Modbus、OPC UA、MQTT等），协议版本统一，确保不同厂商、不同类型的本地组件互联互通；

云端组件兼容性：所有云端组件应适配所选云平台（公有云、私有云、混合云）的技术规范，云服务器、云存储、云数据库、数据分析引擎应支持统一的接口协议，确保云端组件协同工作；云原生应用应支持容器化部署，适配K3s或K8s调度，支持弹性扩展；

本地与云端组件兼容性：本地传输层组件（云端接入网关）与云端云网关应支持统一的传输协议和加密标准，确保本地数据安全传输至云端，云端管控指令可正常下发至本地设备；本地组件应支持云端身份认证，确保接入云端的设备合法性；

跨云平台兼容性：混合云部署模式下，私有云组件与公有云组件应支持跨云数据同步、跨云资源调度，采用统一的数据格式和接口协议，确保混合云架构的协同运行；

软件兼容性：云端应用层软件应适配主流浏览器（Chrome、Edge、Firefox等）和移动端操作系统（Android、iOS），本地采集终端软件应适配本地操作系统，确保用户正常访问和操作；所有软件组件应支持定期升级，且升级后不影响兼容性。

E.3 云单机版（云端单机部署）

云单机版是云部署版的单机形态，核心特点：仅在云端部署一套核心云组件（云服务器、云数据库、云存储等），本地部署感知层和传输层组件，云端单机承担所有数据存储、处理、管控功能，无冗余备份和故障切换能力，架构简单、部署成本低、运维轻量化，适用于小型用能单位、分散用能点位、简易能耗监控场景。

E.3.1 架构拓扑

云单机版架构拓扑简洁，云端组件集中部署，本地组件轻量化部署，具体拓扑如下：

各用能现场感知层（计量器具、传感器、智能设备、采集终端）→ 本地传输层（小型交换机、4G/5G路由器、云端接入网关）→ 公网/专用网络 → 云端单机组件（云服务器、云数据库、云存储、云应用）→ 用户终端（Web端、移动端、大屏端）；安全层组件（云防火墙、云安全中心、本地简易安全设备）覆盖云端和本地，确保全流程安全；云端仅部署一套核心组件，无冗余节点，数据存储在云端云存储，本地采集终端支持断网缓存，联网后自动同步数据至云端，用户通过互联网访问云端应用，实现能源管控。

E.3.2 组件配置标准

云单机版组件配置应满足小型用能场景、分散用能点位的需求，兼顾性价比和轻量化运维，具体配置标准如下：

云端组件：

云服务器：1台弹性云服务器（ECS），CPU≥8核（Intel Xeon或同等性能云服务器），内存≥16GB DDR4，硬盘≥1TB 云SSD + 5TB 云对象存储（OSS），支持按需扩容，部署在单一可用区，具备基础容灾能力；

云数据库：1套关系型云数据库（MySQL 8.0云版） + 1套时序云数据库（InfluxDB 2.0云版），云数据库内存≥8GB，存储容量≥500GB，支持每日自动备份，备份数据存储≥30天；

云应用组件：部署能耗监测、能效优化、设备管控、用户管理等基础云原生应用模块，支持容器化部署，适配云端弹性扩展，无需本地安装；

云安全组件：1套云防火墙、1套云安全中心基础版、1套数据加密服务，支持基础安全防护、数据加密和安全监测功能，符合等保二级合规要求；

云网关：1套云端云网关，支持≤50台本地采集终端同时接入，支持多协议转换和数据加密传输。

本地组件：

感知层组件：根据用能点位数量配置，每个用能现场采集终端≤3台，计量器具≤30台，传感器≤20个，智能设备≤5台，采集终端缓存容量≥8GB，支持断网缓存和加密传输；

传输层组件：每个用能现场部署小型交换机1台（千兆端口≥4个）、4G/5G路由器1台（支持VPN接入）、云端接入网关1台，传输模块根据现场网络环境配置（4G/5G或Wi-Fi）；

安全层组件：每个用能现场部署简易防火墙1台（支持基础包过滤功能），采集终端和云端接入网关支持数据加密和身份认证，确保本地设备安全。

E.3.3 部署流程

云单机版部署流程轻量化、可落地性强，无需搭建本地机房，重点完成云端组件配置和本地组件部署对接，具体流程如下：

云端部署准备：选择适配的云平台（公有云/私有云），完成云账号注册和权限配置，创建云服务器、云数据库、云存储等云端资源，配置云服务器IP地址和安全组，开启云防火墙、数据加密等安全功能；

云端组件部署：在云服务器上部署云网关、大数据分析引擎等平台组件，配置云数据库参数，创建能源管理相关数据库和数据表，设置数据备份策略（每日自动备份）；部署云原生应用组件，配置应用参数，调试云端应用功能；

本地组件部署：在各用能现场安装感知层组件（计量器具、传感器、采集终端）和传输层组件（交换机、4G/5G路由器、云端接入网关），完成硬件连接和调试，确保本地组件运行正常；

本地与云端对接：配置本地云端接入网关参数，接入云端云网关，完成身份认证和协议适配，调试数据传输功能，确保感知层数据可正常上传至云端，云端管控指令可正常下发至本地设备；

安全配置：配置本地简易防火墙规则，开启云端接入网关和云网关的数据加密功能，配置云端身份认证和权限管理，设置安全审计规则，确保全流程安全；

系统调试：整体调试系统，测试数据采集、传输、存储、分析功能，测试云端应用功能和安全防护功能，排查数据传输延迟、连接异常等故障，确保系统运行流畅；

用户培训：对用能单位相关人员进行云端应用操作培训，包括数据查看、设备管控、报表生成、故障处理等，提供线上操作手册；

部署验收：按照本文件规定的测试标准和验收规范，完成部署验收，出具验收报告，验收合格后系统正式投入使用。

E.3.4 适用场景

云单机版适用于用能规模小、用能点位分散、数据量小、无高可用需求，且无本地机房条件、追求轻量化运维、成本优化的场景，具体包括：

小型用能单位（如小型商铺、个体加工厂、小型办公楼），用能点位≤30个，日均数据量≤5万条，无专业运维人员；

分散用能场景（如连锁商铺、分散式写字楼、小型分布式能源站点），用能点位分布在多个区域，需要集中管控且无需本地机房；

简易能耗监控场景（如临时用能场景、小型设备能耗监测），无高可用需求，预算有限，追求快速部署和低成本运维；

对网络依赖度适中，具备公网接入条件，且对数据安全要求适中，无需数据本地化存储的小型用能单位；

初创型用能单位、试点用能项目，需要快速搭建能源管理系统，无需长期投入硬件和运维成本的场景。

E.3.5 维护要求

云单机版维护以云端轻量化运维为主，本地组件维护简易，无需专业运维团队，具体维护要求如下：

云端维护：由云平台服务商和解决方案提供商协同负责，每日监测云端组件（云服务器、云数据库、云应用）运行状态、资源负载情况，查看云端安全日志和数据传输日志，排查异常情况；每周检查数据备份状态，确保备份正常；每月更新云端应用版本，修复软件漏洞，优化应用性能；每季度检查云端安全防护配置，更新安全规则，进行一次安全扫描；

本地维护：安排普通工作人员负责日常维护，每日检查本地组件运行状态、数据采集状态，查看本地传输设备（路由器、云端接入网关）的连接状态，排查断网、设备离线等简单故障；每月检查本地组件线路连接，清理设备灰尘，确保本地组件正常运行；每季度检查本地采集终端缓存情况，清理无效缓存；

故障维护：建立简易故障应急处理机制，接到故障告警后（云端告警、本地告警），本地工作人员先排查本地简单故障（如断网、设备断电），对无法解决的故障及时联系技术支持；云端故障由云平台服务商和技术支持在4小时内完成修复，本地复杂故障由技术支持在8小时内完成修复；故障修复后，应记录故障原因、处理过程和结果，形成故障报告；

数据维护：由解决方案提供商负责，定期清理云端无效数据、冗余数据，确保数据准确性和完整性；每年对云端历史数据进行一次归档，归档数据存储在云对象存储，保留至少3年；定期检查本地与云端数据同步状态，确保数据一致；

用户维护：定期对本地用户进行云端应用操作培训，解答用户操作疑问；根据用户需求，适时调整云端应用参数和功能配置。

E.3.6 局限性

云单机版受限于云端单机部署形态，存在以下局限性，不适用于中大型用能场景、核心用能场景和高可用需求场景：

无冗余备份：仅部署一套云端核心组件，无冗余节点，一旦云端服务器、云数据库出现故障，系统将全面中断，影响能源管理业务；

性能有限：并发处理能力、数据处理能力有限，无法支撑大量用能点位、海量数据的采集和分析，难以适配用能规模扩大和业务需求拓展；

依赖网络：系统运行高度依赖公网或专用网络，一旦网络中断，本地数据无法上传至云端，用户无法远程访问和管控，仅能依靠本地缓存；

扩展受限：云端组件虽支持按需扩容，但单机形态的扩展能力有限，无法支撑大批量采集终端同时接入和复杂数据分析需求；

安全依赖云平台：云端资源和数据的安全高度依赖云平台的安全防护能力，若云平台出现安全漏洞，可能导致数据泄露或云端资源被入侵。

E.4 云高可用集群版

云高可用集群版是云部署版的集群形态，核心特点：在云端部署多套核心云组件（节点），通过云集群管理技术实现负载均衡、故障切换、冗余备份，本地部署感知层和传输层组件，支持多可用区部署，具备高可靠性、高可用性、高处理能力、弹性扩展能力，运维轻量化、集中管控能力强，适用于中大型用能单位、分散用能点位、跨区域管理、核心用能场景。

E.4.1 架构拓扑

云高可用集群版架构拓扑采用云端多节点集群部署、多可用区备份，本地组件分布式部署，核心组件冗余配置，具体拓扑如下：

各用能现场感知层（计量器具、传感器、智能设备、采集终端）→ 本地传输层（小型交换机、4G/5G路由器、云端接入网关）→ 公网/专用网络（VPN/专线）→ 云端集群组件（云服务器集群、云数据库集群、云存储集群、云应用集群）→ 用户终端（Web端、移动端、大屏端）；安全层组件（云防火墙集群、云安全中心、本地简易安全设备）覆盖云端和本地，确保全流程安全；云端集群采用多可用区部署（至少2个可用区），各节点通过云集群管理软件连接，实现负载均衡和故障切换，数据存储在云存储集群，支持多可用区冗余备份；本地采集终端支持断网缓存，联网后自动同步数据至云端集群；用户通过互联网访问云端应用集群，实现多区域、多场景集中管控，架构符合“云-边-端”协同的云部署适配要求。

云端集群部署模式支持两种拓扑：主备模式、负载均衡模式，可根据用能场景和高可用需求选择：

主备模式：1个主可用区（部署主节点）、≥1个备可用区（部署备节点），主节点承担主要业务（数据存储、处理、管控），备节点处于待命状态，主节点或主可用区故障时，备节点自动切换，接管主节点业务，切换过程无人工干预；

负载均衡模式：≥3个节点（分布在≥2个可用区），所有节点同时承担业务，云集群管理软件将用户访问、数据处理任务均匀分配到各节点，实现负载均衡，单个节点或单个可用区故障时，其他节点自动接管其业务，不影响系统正常运行。

E.4.2 节点配置标准

云高可用集群版节点配置应满足中大型用能场景、分散用能点位、跨区域管理的需求，核心节点冗余配置、多可用区部署，具体配置标准如下（以3节点负载均衡模式、2个可用区为例）：

云端组件：

云服务器集群：3台弹性云服务器（ECS），分布在2个可用区（可用区A：2台，可用区B：1台），每台云服务器配置：CPU≥16核（Intel Xeon或同等性能云服务器），内存≥32GB DDR4，硬盘≥2TB 云SSD + 10TB 云对象存储（OSS），支持双可用区部署，具备弹性扩容能力，应符合 GB/T 21028 的规定；

云存储集群：1套云磁盘阵列（存储容量≥20TB，支持RAID 5/6冗余备份） + 1套云对象存储（OSS，存储容量≥50TB），支持多可用区备份，存储速率≥2 000 MB/s，支持数据生命周期管理；

云数据库集群：3台云数据库服务器（分布在2个可用区），部署主从复制架构（MySQL云集群）或分布式数据库（InfluxDB云集群），每台云数据库内存≥16GB，存储容量≥1TB，支持数据实时同步，主节点故障时，从节点自动切换，确保数据库可用性；

云应用集群：部署能耗监测、能效优化、设备管控、碳排放管理等全套云原生应用模块，支持容器化部署（Docker+K8s），分布在3台云服务器，支持负载均衡和故障自动切换；

云集群管理组件：1套云集群管理软件（如K8s、云原生集群管理平台），负责集群节点调度、负载均衡、故障切换、扩容缩容管理，实时监测集群节点运行状态；

云安全集群：2套云防火墙（分布在2个可用区）、1套云安全中心企业版、1套数据加密服务企业版、1套身份认证服务企业版，支持DDoS高防、入侵防御、数据脱敏、多因素认证等功能，符合等保三级合规要求；

云网关集群：3套云端云网关（分布在2个可用区），支持≤500台本地采集终端同时接入，支持多协议转换、数据加密传输和身份认证，确保本地与云端的稳定交互。

本地组件：

感知层组件：根据用能点位数量配置，每个用能现场采集终端≤10台，计量器具≤100台，传感器≤50个，智能设备≤20台，采集终端缓存容量≥32GB，支持断网缓存、加密传输和集群接入；总采集终端≤500台，总用能点位≤5000个；

传输层组件：每个用能现场部署小型交换机1台（千兆端口≥8个）、4G/5G路由器1台（支持VPN/专线接入）、云端接入网关1台，重要用能现场采用双链路传输（4G/5G+专线），避免单条链路故障导致数据传输中断；传输模块根据现场网络环境配置，确保数据传输稳定；

安全层组件：每个用能现场部署简易防火墙1台（支持包过滤、入侵检测功能），采集终端和云端接入网关支持数据加密、身份认证和异常监测，重要用能现场部署加密设备，确保本地设备和数据安全。

E.4.3 集群部署策略

云高可用集群版部署策略重点关注云端多可用区部署、负载均衡、故障切换、冗余备份，确保集群高可用性和弹性扩展能力，同时兼顾本地组件分布式部署和数据安全传输，具体部署策略如下：

云端集群部署：云端所有核心组件（云服务器、云数据库、云存储、云应用、云网关）采用多可用区部署（至少2个可用区），可用区之间地理位置独立、基础设施隔离，避免单一可用区故障影响整个集群；集群节点配置一致，确保节点协同工作；

集群管理：部署云原生集群管理软件（K8s），配置负载均衡策略（轮询、加权轮询），实现用户访问、数据处理任务的均匀分配；配置故障检测机制，实时监测各节点、各可用区的运行状态（CPU、内存、硬盘、网络、软件运行状态），监测频率≤5秒/次；

故障切换：配置自动故障切换策略，主备模式下，主节点或主可用区故障时，备节点在≤30秒内自动切换，接管主节点的IP地址、业务进程和数据处理任务；负载均衡模式下，单个节点故障时，集群管理软件立即停止向故障节点分配任务，将未完成的任务和新任务均匀分配至其他正常节点，单个可用区故障时，其他可用区的节点自动接管其业务，切换过程无感知，不影响用户使用和数据采集；

数据备份：采用“多可用区备份+跨区域备份”双重备份策略，云数据库集群支持主从复制，数据实时同步至不同可用区；云存储集群支持多可用区冗余，确保单块硬盘、单个可用区故障时数据不丢失；每日自动进行全量备份，每小时进行增量备份，备份数据存储在不同可用区和跨区域备份中心，保留至少5年；

网络部署：本地与云端采用专用网络（VPN/专线）为主、公网（4G/5G）为备用的双链路传输模式，确保数据传输稳定；云端配置网络负载均衡，优化数据传输效率；本地传输层采用VLAN划分，隔离不同用能现场的数据，提升网络安全性；

软件部署：所有云端节点部署相同版本的平台软件、应用软件、安全软件，软件参数统一配置，采用容器化部署和灰度更新策略，实现软件的统一安装、更新和回滚，避免更新过程影响集群正常运行；本地组件软件采用批量部署工具，实现统一安装和更新；

弹性扩展：配置自动扩容缩容策略，根据云端资源负载情况、数据量增长情况，自动调整云服务器、云存储、云数据库的配置和数量，高峰时段自动扩容，低谷时段自动缩容，优化资源利用率，降低运维成本；支持本地采集终端的灵活扩容，无需调整云端集群核心配置。

E.4.4 故障切换机制

云高可用集群版故障切换机制采用“实时监测、自动告警、自动切换、故障恢复和集群自愈”的闭环机制，结合多可用区部署优势，确保故障快速处理、业务不中断，具体如下：

故障监测：云集群管理软件、云安全中心实时监测各节点、各可用区的运行状态（CPU使用率、内存使用率、硬盘存储空间、网络连接状态、软件运行状态），监测频率≤5秒/次；同时监测本地与云端的数据传输流程、数据采集流程，实时监测云端资源负载情况，发现异常（节点故障、可用区故障、网络中断、数据传输异常）立即触发告警；

故障告警：故障发生时，系统自动发出分级告警（紧急告警、普通告警），包括声音告警、短信告警、平台告警、邮件告警，告知维护人员故障节点、故障类型、故障时间、故障影响范围，告警信息同步存储在云端安全日志中，便于后续复盘；

自动切换：根据集群部署模式（主备/负载均衡）和故障类型，自动触发故障切换流程：

单个节点故障：负载均衡模式下，集群管理软件立即停止向故障节点分配任务，将未完成的任务和新任务均匀分配至其他正常节点，切换延迟≤10秒；主备模式下，备节点立即接管主节点业务，切换延迟≤30秒；

单个可用区故障：集群管理软件立即将故障可用区的所有业务、数据处理任务，转移至其他正常可用区的节点，实现可用区间的故障切换，切换延迟≤60秒，不影响业务连续性；

网络故障：本地与云端单条链路故障时，自动切换至备用链路（公网/专线），数据传输不中断；云端内部网络故障时，集群管理软件自动调整网络路由，确保节点间数据同步正常。

故障恢复：维护人员接到告警后，根据故障类型和分级，快速排查故障原因（云端节点故障、可用区故障、网络故障、本地设备故障），完成故障修复；云端节点故障修复后，集群管理软件自动检测节点状态，确认正常后，将节点重新加入集群，分配业务任务；可用区故障修复后，自动同步数据至该可用区，恢复集群完整负载能力；故障修复过程应记录在故障报告中；

集群自愈：配置集群自愈功能，对于轻微故障（如节点临时离线、软件重启故障），集群管理软件自动尝试修复，无需人工干预；修复成功后，自动恢复节点业务，确保集群持续稳定运行。

E.4.5 适用场景

云高可用集群版适用于用能规模大、用能点位多且分散、跨区域管理、对系统可用性和集中管控能力要求高，且无本地机房条件、追求轻量化运维的中大型用能单位、核心用能场景，具体包括：

中大型工业企业、集团型企业，用能点位≥500个，日均数据量≥100万条，用能点位分布在多个区域，需要跨区域集中管控，核心生产环节依赖能源管控，不允许系统中断；

大型产业园区、工业园区、经济开发区，涵盖多家用能单位，用能类型复杂（电力、水、燃气、热力、可再生能源等），用能点位分散，需要集中管控且追求轻量化运维；

跨区域经营的商业连锁企业、物流园区，用能点位分布在多个城市，需要统一的能源管理平台，实现能耗集中监测、统一管控和能效优化；

核心用能场景（如大型数据中心、新能源电站、城市供热系统），能源管控直接影响核心业务运行，应具备高可用性、高可靠性和弹性扩展能力；

对网络依赖度较高，具备公网和专用网络接入条件，对数据安全要求高（符合等保三级），且无本地机房条件、追求运维效率和成本优化的用能单位，符合《能源行业数据安全管理办法（试行）》《中华人民共和国数据安全法》等相关要求。

E.4.6 维护要求

云高可用集群版维护以云端自动化运维为主、本地轻量化运维为辅，依托云原生技术实现集群自愈与批量管理，重点保障多可用区集群协同、数据跨区同步及本地云端链路稳定，同时符合等保三级、数据安全法相关合规要求，具体维护要求如下：

云端运维（核心运维层）

云端运维由解决方案提供商联合云平台服务商实施，采用“自动化监测+分级响应+灰度操作”模式，具体要求：

日常自动化监测

依托云集群管理平台（K8s）和云安全中心，实现集群节点、云数据库、云存储、云网关的7×24 h实时监测，监测指标含CPU/内存/磁盘负载、数据同步状态、链路连通性、安全漏洞、容器健康度，监测频率≤5秒/次。

配置自动化告警规则，对指标阈值超标（如节点负载≥80%）、数据同步延迟＞10秒、可用区链路中断等异常，自动触发分级告警（紧急/重要/普通），告警方式含短信、邮件、平台弹窗、企业微信/钉钉通知，紧急告警响应时限≤5分钟。

定期维护（按周期执行）

表 E.1　云高可用集群版定期维护要求

维护周期	核心维护内容	执行要求
每日	数据备份校验、集群自愈检查、安全日志审计	自动完成，生成日报，异常项标注处理
每周	云应用版本灰度更新、漏洞扫描、负载均衡策略优化	非高峰时段（00:00-04:00）执行，保留回滚预案
每月	多可用区故障切换演练、数据库性能调优、安全策略更新	演练过程不影响业务，形成演练报告

表 E.1　云高可用集群版定期维护要求（续）

维护周期	核心维护内容	执行要求

维护周期	核心维护内容	执行要求
每季度	跨区域备份恢复测试、集群扩容缩容压力测试、合规性自查	测试覆盖全业务流程，自查结果符合等保三级要求
每年	云端资源全量巡检、老旧组件升级、安全合规审计	联合第三方机构完成，出具审计报告

故障运维

建立分级故障处理机制：紧急故障（如可用区宕机、集群崩溃）启动应急响应，技术团队≤30分钟到场，≤1小时恢复核心业务；重要故障（如单节点宕机、数据同步异常）≤2小时修复；普通故障（如非核心应用卡顿）≤4小时修复。

故障修复后，应完成“故障定位、原因分析、修复方案和预防措施”闭环，形成故障分析报告，纳入运维知识库，避免同类问题重复发生。

本地运维（边缘运维层）

本地运维由用能单位安排专人负责，无需专业运维资质，重点保障本地感知层、传输层组件正常运行及链路通畅，具体要求：

日常维护

每日查看本地采集终端、云端接入网关、4G/5G路由器的运行状态（电源、指示灯、连接状态），记录数据采集是否正常，发现设备离线、断网等情况，先执行基础排查（重启设备、检查线路、确认网络信号）。

每周清理本地设备灰尘，检查线路连接是否松动，核对4G/5G流量使用情况，确保不出现流量耗尽导致的传输中断。

定期维护

每月配合云端运维团队，完成本地组件固件的批量升级（由云端推送，本地一键确认），升级后测试数据上传与指令接收功能。

每季度检查本地简易防火墙规则是否有效，更换老化的传输线路和电源适配器，对采集终端缓存进行清理优化。

故障协同处理

本地排查无法解决的故障（如采集终端损坏、网关无法接入云端），需立即联系技术支持，提供设备编号、故障现象、现场网络情况等信息，配合技术人员完成远程或现场修复。

故障修复后，在本地运维台账中记录故障详情、处理过程及结果，确保运维全流程可追溯。

数据运维（合规核心层）

数据运维贯穿云端与本地，重点保障数据全生命周期的准确性、完整性、安全性、合规性，具体要求：

数据同步管理

云端自动监测本地与云端的数据同步状态，断网恢复后，确保本地缓存数据断点续传，无重复、无丢失，同步完成后生成同步报告。

每月核对云端数据与本地计量器具原始数据，确保数据准确率≥99.95%，发现数据偏差立即排查原因（如采集终端故障、传输丢包）并修正。

数据存储与归档

云端按照“热数据（近3个月）-温数据（3个月-1年）-冷数据（1年以上）”分层存储，热数据存于云SSD，保障查询效率；冷数据归档至云对象存储，降低存储成本，归档数据保留至少5年，符合行业数据留存要求。

每年完成冷数据归档校验，确保归档数据可正常读取、恢复，归档记录纳入合规审计材料。

数据安全运维

定期更新数据加密密钥，每季度检查数据传输加密（SSL/TLS 1.3）、存储加密（SM4）是否生效，确保敏感数据（如用能核心数据、碳排放数据）全程加密。

严格管控数据访问权限，每月审计用户数据访问日志，发现越权访问、异常批量下载等行为，立即暂停用户权限并开展安全核查。

运维台账管理

云端与本地均应建立电子运维台账，云端台账包含集群节点信息、资源配置记录、版本更新记录、故障处理记录、安全审计记录、数据备份记录；本地台账包含设备清单、设备运维记录、链路检查记录、故障协同记录。

运维台账实时更新，保存期限≥5年，可随时调取查阅，作为合规检测、故障复盘、责任认定的重要依据。

支持运维台账导出功能，导出格式兼容Excel、PDF，满足监管部门检查、审计机构审核的需求。

局限性

云高可用集群版虽具备高可用性、弹性扩展等核心优势，但受部署形态、网络环境、政策要求等因素限制，存在以下局限性，应结合实际场景评估选用：

网络依赖性强：核心业务（远程管控、实时数据分析、跨区域协同）高度依赖公网+专用网络双链路，若出现区域性网络故障（如运营商基站宕机、专线中断），即使本地具备缓存能力，也无法实现远程实时管控和数据实时分析。

合规适配限制：对于国家或行业明确要求“核心数据100%本地化存储”的场景（如部分军工、能源核心企业），即使采用混合云部署，也可能无法完全满足合规要求，应优先选择本地高可用集群版。

运维技术门槛较高：云端集群的深度运维（如K8s集群调优、分布式数据库性能优化、多可用区容灾策略调整）需专业云原生技术团队支撑，用能单位若选择自主运维，需投入成本培养专业人才。

成本相对较高：多可用区部署、云安全企业版、专用网络专线等配置，导致云端资源租赁、网络使用的整体成本高于云单机版，对于小型用能单位，性价比偏低。

跨云适配复杂度高：若采用混合云部署，私有云与公有云的跨云数据同步、跨云资源调度需解决接口兼容、数据格式统一、安全策略协同等问题，部署与维护的复杂度显著提升。